

ЗМІСТ

CONTENTS

| | |
|---|--|
| <i>Василий Алексеев, Юлия Синица, Денис Горелов</i> Модифицированный метод диграфов в задаче аутентификации пользователей по клавиатурному почерку..... 252 | <i>Vasyl Aliexsieiev, Yuliia Synytsia, Denis Gorelov</i> Modified digraphs method in the problem of authenticating users using keystroke dynamics..... 252 |
| <i>Антон Олексійчук</i> Достатня умова стійкості SNOW 2.0-подібних потоків шифрів відносно певних атак зі зв'язаними ключами 261 | <i>Anton Alekseychuk</i> Sufficient condition for SNOW-2.0-like stream ciphers' to be secure against some related key attacks..... 261 |
| <i>Олександр Кузнецов, Андрій Пушкар'юв, Олексій Шевцов, Тетяна Кузнецова</i> Несиметричне криптографічне перетворення з використанням алгебраїчних блокових кодів..... 269 | <i>Oleksandr Kuznetsov, Andriy Pushkarev, Oleksiy Shevtsov, Tetjna Kuznetsova</i> Public-key code-based cryptography..... 269 |
| <i>Любовь Рябова, Мария Самойленко, Юлия Бойко</i> Препарирование изображений радужки при идентификации личности..... 276 | <i>Lyubov Ryabova, Maria Samoylenko, Yuliia Boiko</i> Iris in images preparation identification..... 276 |
| <i>Анатолий Белецкий, Владимир Лужецкий</i> Синтез симметричных систем функций золотого сечения..... 283 | <i>Anatoly Beletsky, Volodymyr Luzhetsky</i> Synthesis of symmetrical functions of golden ratio 283 |
| <i>Олександр Кузнецов, Юрій Горбенко, Олексій Шевцов, Тетяна Кузнецова</i> Дослідження криптографічних атак на схеми електронного цифрового підпису в фактор- кільцях зрізаних поліномів 293 | <i>Oleksandr Kuznetsov, Yurii Gorbenko, Oleksiy Shevtsov, Tetjna Kuznetsova</i> Study of cryptographic attacks on the digital signature scheme in quotient ring of truncated polynomials 293 |
| <i>Антон Олексійчук, Юрій Сергієнко</i> Неасимптотичні оцінки ймовірності правильного відновлення повідомлень у двійковому відвідному каналі зі стиранням..... 301 | <i>Anton Alekseychuk, Yurii Serhiienko</i> Non-asymptotic estimates for the probability of correct messages recovering in the binary erasure wiretap channel..... 301 |
| <i>Андрей Фесенко</i> Критерий обнаружения как влияющий фактор объема базы данных, биометрических систем контроля доступа..... 308 | <i>Andrey Fesenko</i> Detection criterion as the influencing factor of the database size for biometric access control systems..... 308 |
| <i>Александр Корченко, Светлана Казмирчук, Юрий Дрейс, Андрей Гололобов</i> Бистабильная интегрированная кортежная модель характеристик риска..... 314 | <i>Oleksandr Korchenko, Svitlana Kazmirchuk, Yurii Dreis, Andrew Gololobov</i> Bistable and integrated based tuple model of risk characteristics..... 314 |
| <i>Володимир Чуприн, Володимир Вишняков, Михайло Пригара</i> Генерування випадкових чисел штатними засобами хостів мережі інтернет..... 323 | <i>Volodymyr Chupryn, Volodymyr Vysniakov, Mykhailo Prygara</i> Method of generation of casual numbers on the basis of the use of apparatus of the computer plugged in the internet..... 323 |
| <i>Степан Винничук, Александр Корнейко, Евгений Максименко</i> Методы извлечения корня с остатком из многозначных чисел для решения задач асимметричной криптографии..... 336 | <i>Stepan Vinnichuk, Oleksandr Korneiko, Yevgen Maksymenko</i> Methods of extracting root with the residues from multi-bit numbers to meet the challenges of asymmetric cryptography..... 336 |